Overview of Cybersecurity Automation Sub-Project (CASP) June 2023 Cybersecurity Automation Village

Charlie Frick

IOB Working Group Meeting

July 2023

Note: Selected slides copied from CASP Village Summary presentation that will be released later by CASP team

Overview

- On June 13, 2023, CASP hosted a cybersecurity automation village / plugfest
- Event was hybrid with virtual participants and in-person at University of Southern California
  - Event was run in conjunction with CISA “SBOM-A-RAMA”
- This talk will provide an overview of the event and capabilities demonstrated
- Plugfest information available at: https://github.com/opencybersecurityalliance/casp/tree/main/Plugfests/NextPlugfest/2023-06-13-USC

Participants

Participant technologies demonstrated

OpenC2 demonstration overview

OpenC2 Nuts and Bolts

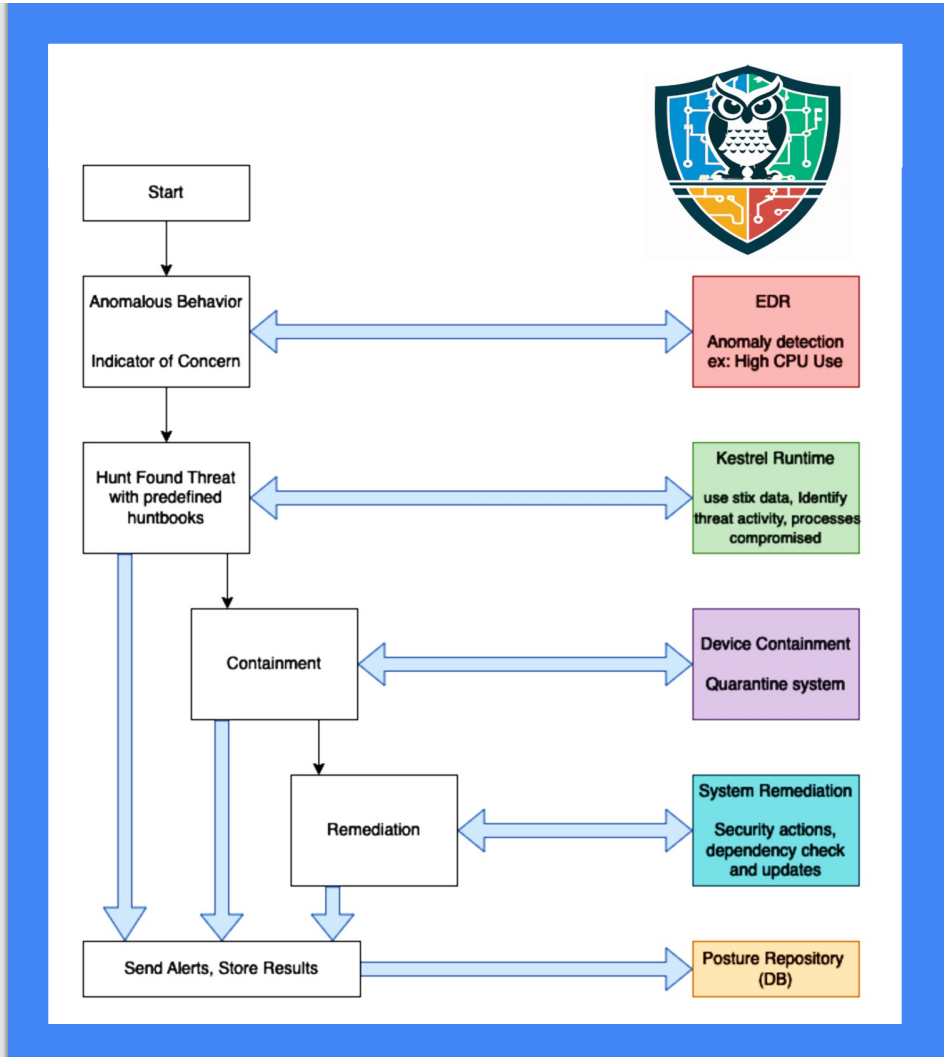
- **Orchestrator** controls **cybersecurity services**
- **Actuator Profile** for each service is an **open** standard for control messages
- **Schema** specifies AP content and validates messages
- **JADN Repository** contains schemas, test messages and Python scripts to support AP authoring, device development, and plugfest testing

https://github.com/oasis-open/openc2-jadn-software

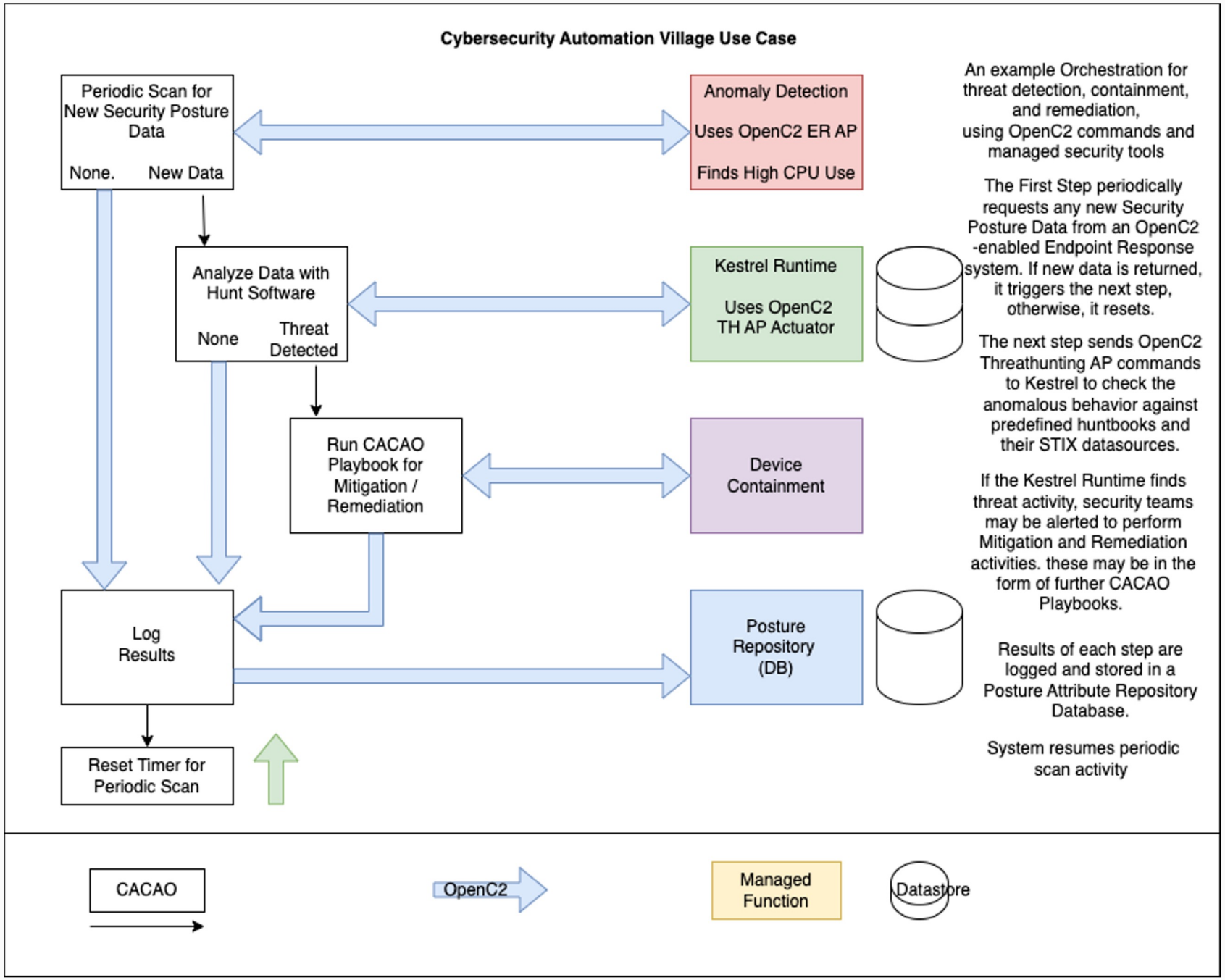
- **MQTT Broker** facilitates remote device development and virtual plugfest participation

START EARLY for next time!

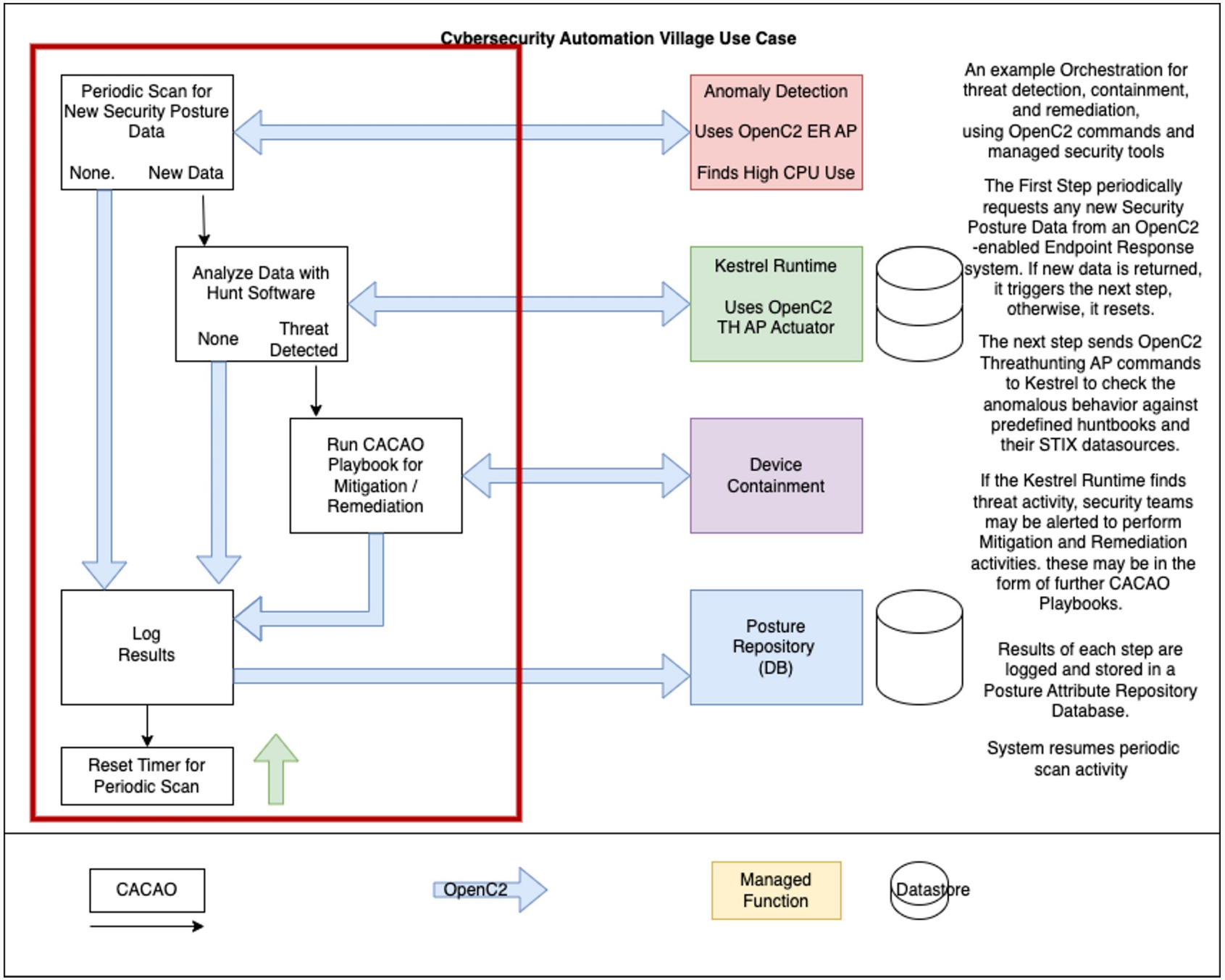
https://github.com/opencybersecurityalliance/casp/blob/main/Plugfests/NextPlugfest/2023-06-13-USC/SweatEquity/openc2-mqtt-topics.md



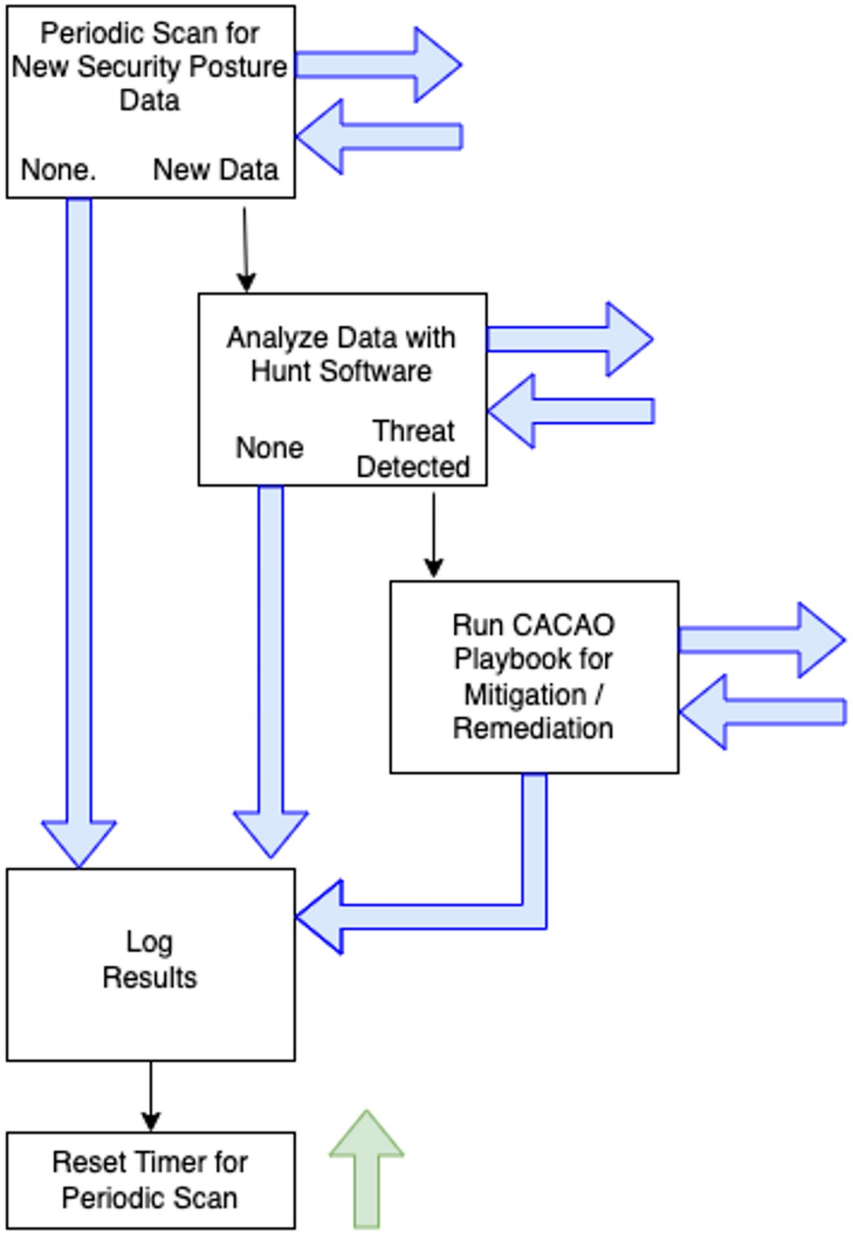
Thousand Foot View



CACAO Orchestrates OpenC2



Cybersecurity Automation Village Use Case

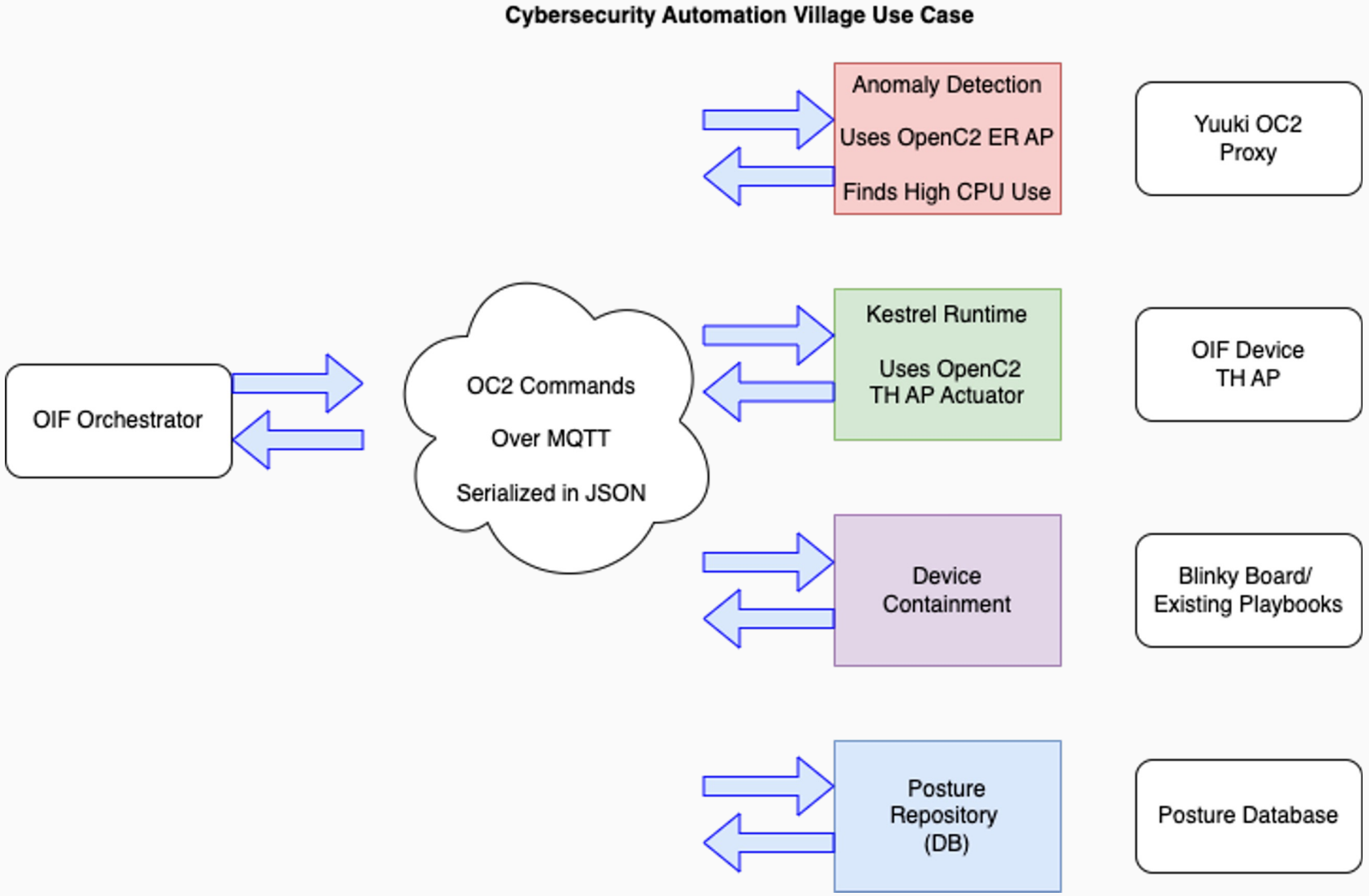


Playbook 1
Send OC2 command in ER AP on oc2/cmd/er
  Wait n seconds for response on oc2/rsp/er
  Handle Response
  Store response data
    if response is empty, repeat immediately
    if response does not contain new data, repeat in an hour
    if response contains new data, Trigger playbook2

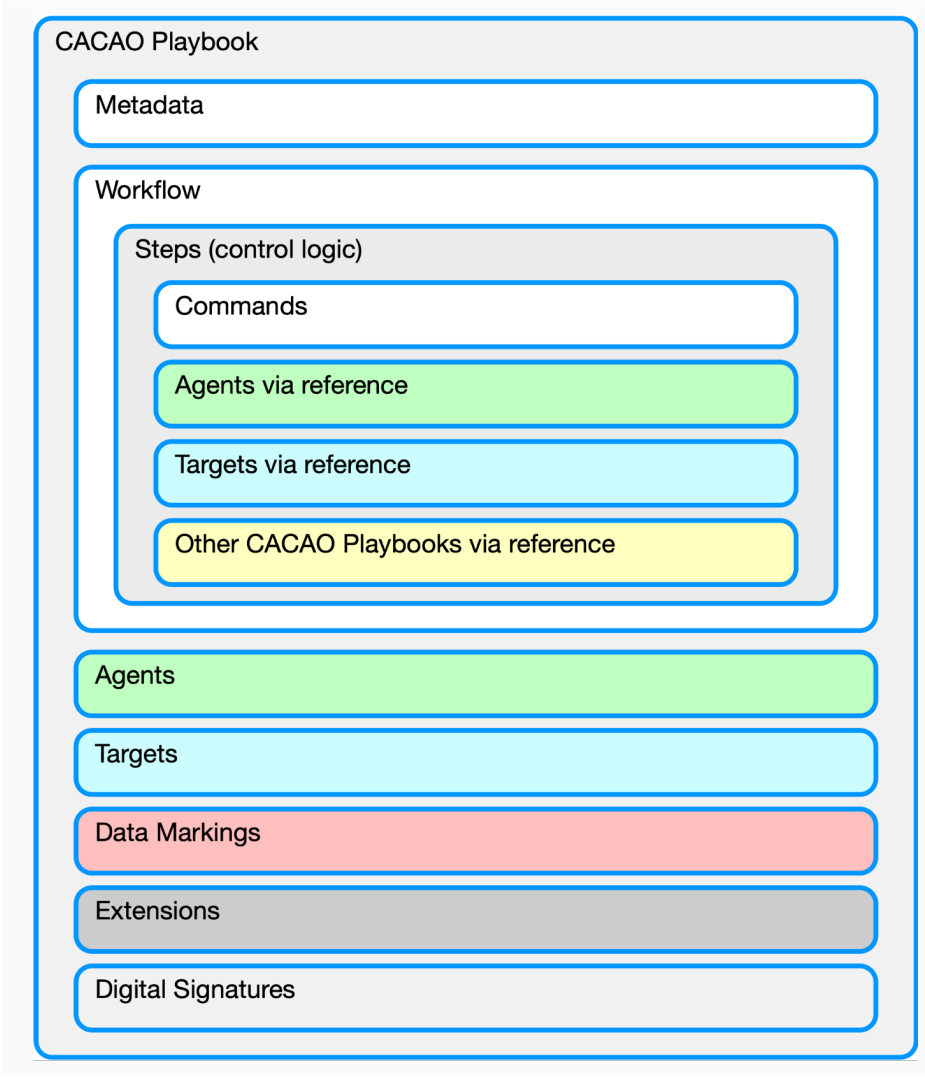
Playbook 2
Send OC2 command in TH AP on oc2/cmd/th
  Wait n seconds for response on oc2/rsp/th
  Handle Response
  Store response data
    if response like "X", ransomware indicated, Trigger playbook3
    if response like "Y", something else indicated, Trigger playbook4
    else, pass back to playbook1

Playbook 3
Send OC2 command in Blinky AP
  when initiated by security team, perform mitigation/ remediation

Today's Implementations



CACAO Overview

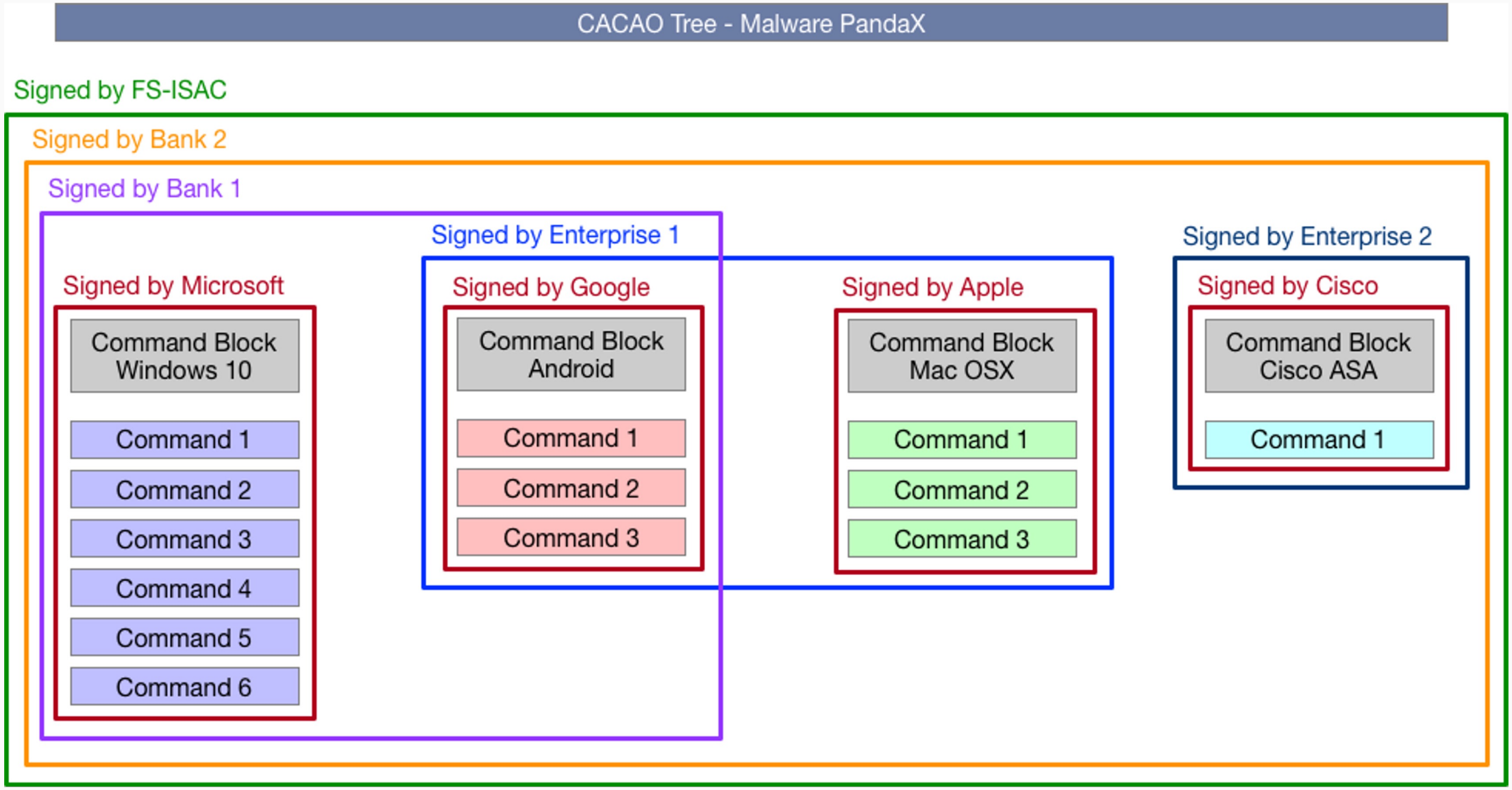


Overview

CACAO is a machine readable schema for defining and exchanging/sharing cyber security playbooks and workflows.

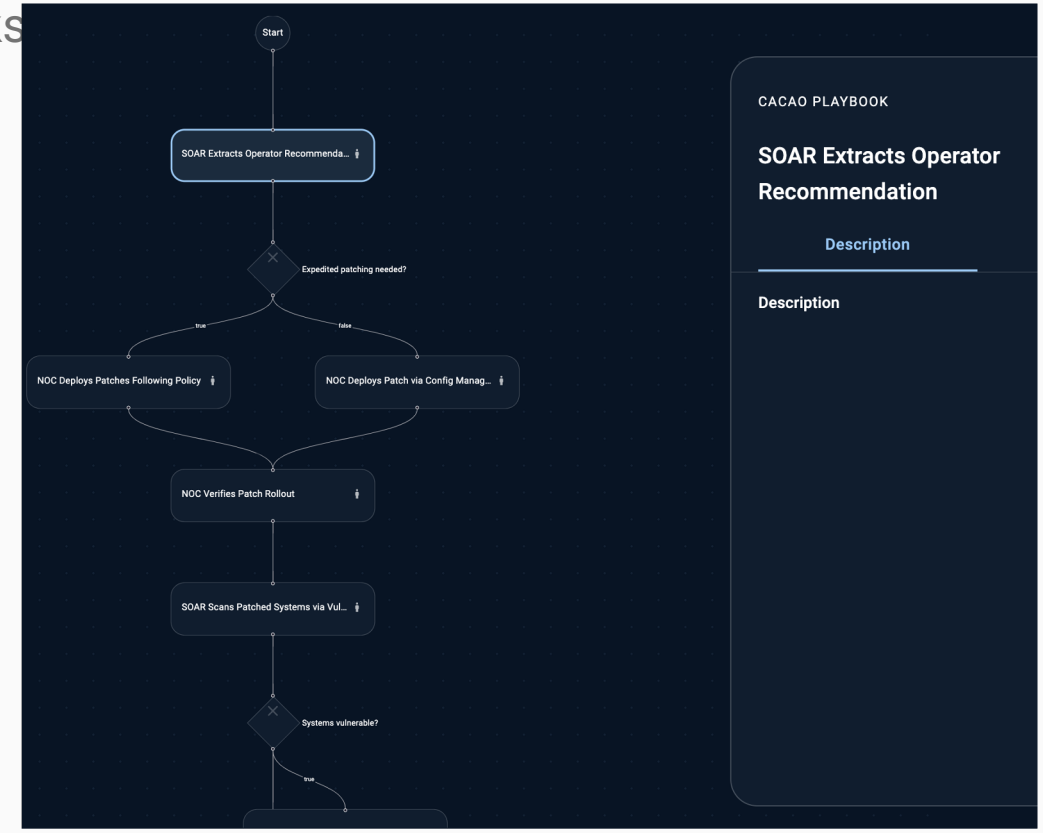
The specification describes how these playbooks can be created, documented, and shared in a structured and standardized way across organizational boundaries and technological solutions.

Digital Signatures



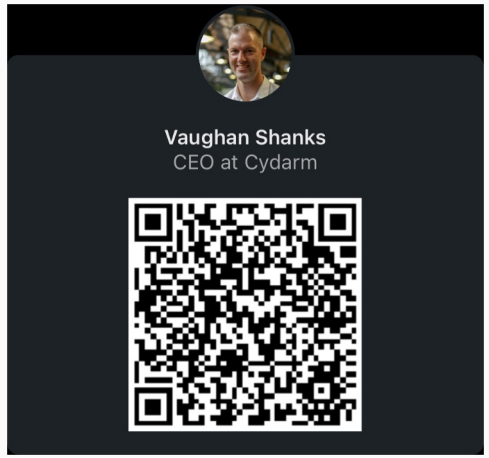
CACAO Playbooks - Observations and Lessons Learned

- Cydarm has integrated CACAO playbooks into cyber ops case management platform
- Playbooks represent processes rather than activities / tasks => human in the loop
- Goal: manual => hybrid => fully automated
- Challenges:
  - Reusable steps / composability - how?
  - The difference between shareable tradecraft vs executable workflows
  - State management and reentrant workflows
- Security
  - Command injection
  - Tradecraft confidentiality



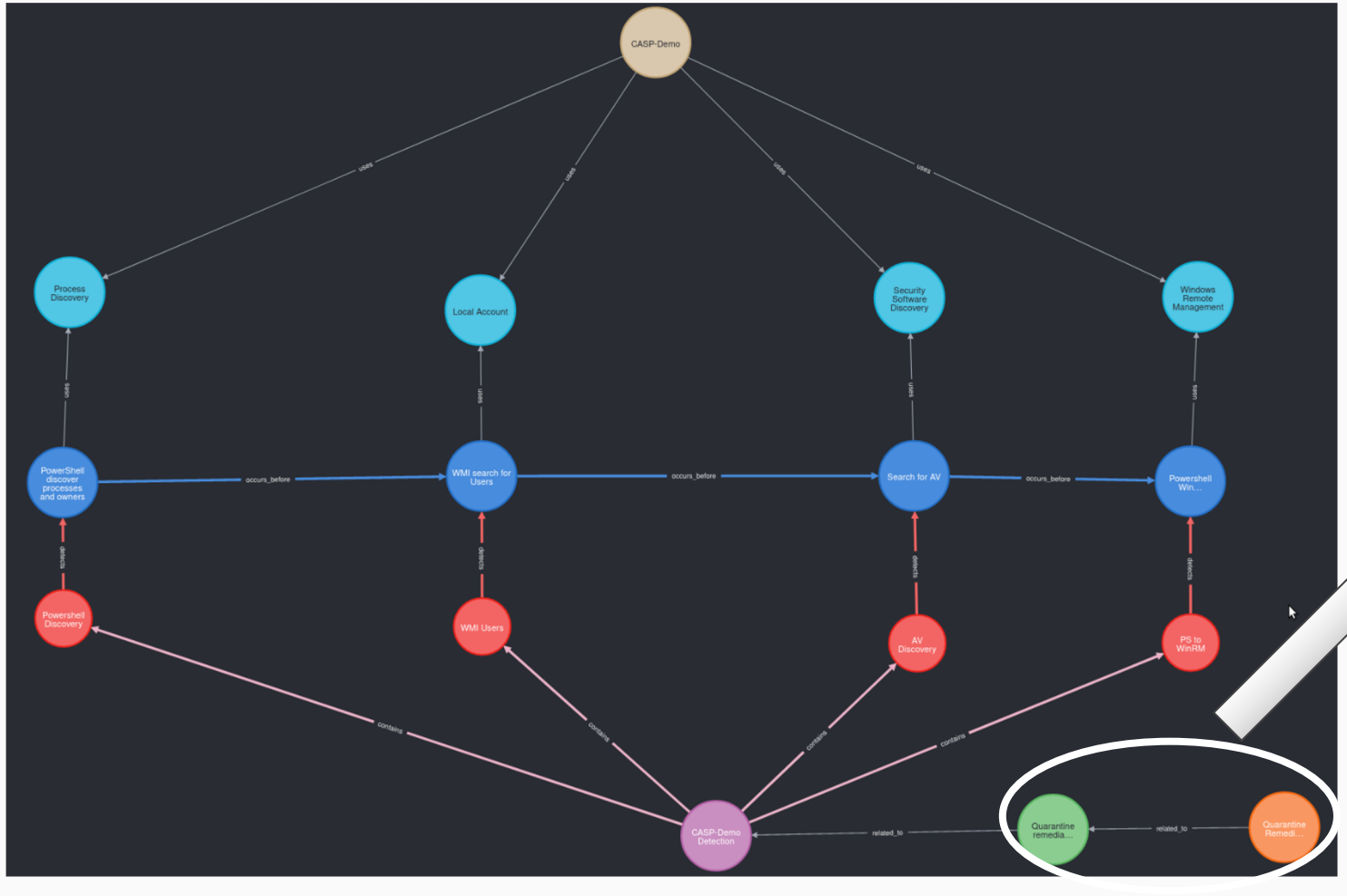
BPMN-to-CACAO Open Source

- Goal: build software to execute CACAO playbooks
- Problem: no repository of CACAO examples!?!
- 81 existing playbooks written by CISA in BPMN
  - https://github.com/cisagov/shareable-soar-workflows
- Why not convert BPMN XML to CACAO JSON?
  - **https://github.com/cydarm/bpmn-to-cacao released 12 June 2023 (yesterday!)**
  - Now we have many CACAO examples!
- Challenges:
  - Some control structures are not yet well handled
  - CACAO logic uses procedural programming norms, BPMN does not, e.g. “gateways” - translation compatibility issues
  - Still need to add OpenC2 or similar to automates steps
- Contributions welcomed!

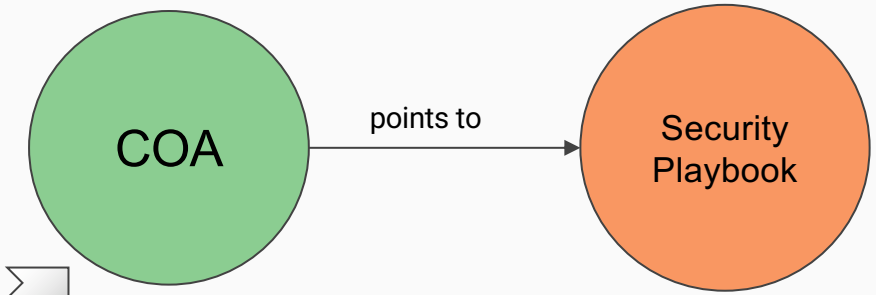


Coupling and Sharing Playbooks with CTI - STIX 2.1 Use Case

Cutting Corners: use case will be presented later by the OCA IOB subproject



STIX 2.1 Objects



Extension Definition

Extension available on GitHub - Work in Progress: https://github.com/cyentific-rni/stix2.1-coa-playbook-extension

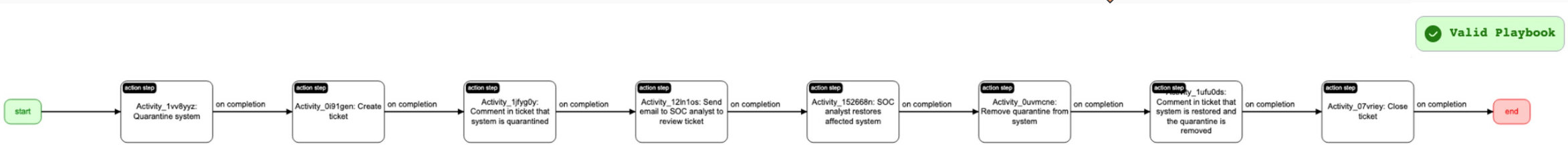
Generating|Modifying|Visualizing CACAO Playbooks

CACAO Security Playbook


```
{
    "type": "playbook",
    "spec_version": "cacao-2.0",
    "id": "playbook--767d859e-7387-4e0c-95c0-458ca369486f",
    "name": "Process_1811f8w: Quarantine and Remediate",
    "playbook_types": [
        "mitigation",
        "remediation"
    ],
    "created_by": "identity--b085a68a-bf48-4316-9667-37af78cba894",
    "created": "2022-03-31T13:00:00.000Z",
    "modified": "2022-03-31T13:00:00.000Z",
    "workflow_start": "start--ece532df-970a-417c-a125-5e7713e10f7c",
    "workflow": {
        "start--ece532df-970a-417c-a125-5e7713e10f7c": {
            "name": "StartEvent_1: System Course of Action Alert",
            "on_completion": "action--d22408fc-a99c-4c45-8770-27dac6df293a",
            "type": "start"
        },
        "end--4d3134d9-68d2-4bde-87ca-a5bfe8468aa6": {
            "name": "Event_17zpsn5: End",
            "type": "end"
        },
        "action--d22408fc-a99c-4c45-8770-27dac6df293a": {
            "name": "Activity_1vv8yyz: Quarantine system",
            "on_completion": "action--d1d15ab7-b557-4f82-8d9b-495438a5c9a9",
            "type": "action",
            "commands": [
                {
                    "type": "http-api"
                }
            ]
        },
        "action--d1d15ab7-b557-4f82-8d9b-495438a5c9a9": {
            "name": "Activity_0i91gen: Create ticket",
            "on_completion": "action--3efbe056-6d1e-4407-89bb-bb54016d9dea",
            "type": "action",
            "commands": [
                {
                    "type": "http-api"
                }
            ]
        },
        "action--3efbe056-6d1e-4407-89bb-bb54016d9dea": {
            "name": "Activity_1jfyg0y: Comment in ticket that system is quarantined",
            "on_completion": "action--27f8278c-8b87-4815-8f40-9c6af610203e",
            "type": "action",
            "commands": [
```


Time for demo?

CACAO JSON Validation Schemas: https://github.com/cyentific-rni/cacao-json-schema



TAC Ontology Overview

Overview

The Threat Actor Context (TAC) ontology is a community-driven project led by the OASIS Threat Actor Context Technical Committee. The TAC ontology is a knowledge representation framework focused on comprehensively representing the context around adversaries. The project comprises a set of concept definitions and their relationships encoded in Web Ontology Language (OWL) that altogether harmonize into what we call the Threat Actor Context ontology.

- Exchange Format to Analysis Format
  - STIX 2.1 Specification to STIX 2.1 Ontology
    - Separates the Data from the Model
- STIX JSON to STIX Knowledge Graph
- Formal Logic
  - New Facts from Existing Facts
  - From Implicit Knowledge to Explicit
- Classifying Threat Actors Analysis
  - Use Case: Intel Threat Agent Library (TAL)

Automate Analysis & Reduce Cognitive Load

Exchange

Analysis
&
Reasoning

TAC
Ontology

New Facts

Semantic Interoperability

Exchange Format to Graph Analysis Format

STIX Version 2.1

docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_t56pn7elv6u7

OASIS OPEN

STIX Version 2.1

OASIS Standard

10 June 2021

This stage:
https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.docx (Authoritative)
https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html
https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.pdf

Previous stage:
https://docs.oasis-open.org/cti/stix/v2.1/cs02/stix-v2.1-cs02.docx (Authoritative)
https://docs.oasis-open.org/cti/stix/v2.1/cs02/stix-v2.1-cs02.html
https://docs.oasis-open.org/cti/stix/v2.1/cs02/stix-v2.1-cs02.pdf

Latest stage:
https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.docx (Authoritative)
https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html
https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.pdf

Technical Committee:
OASIS Cyber Threat Intelligence (CTI) TC

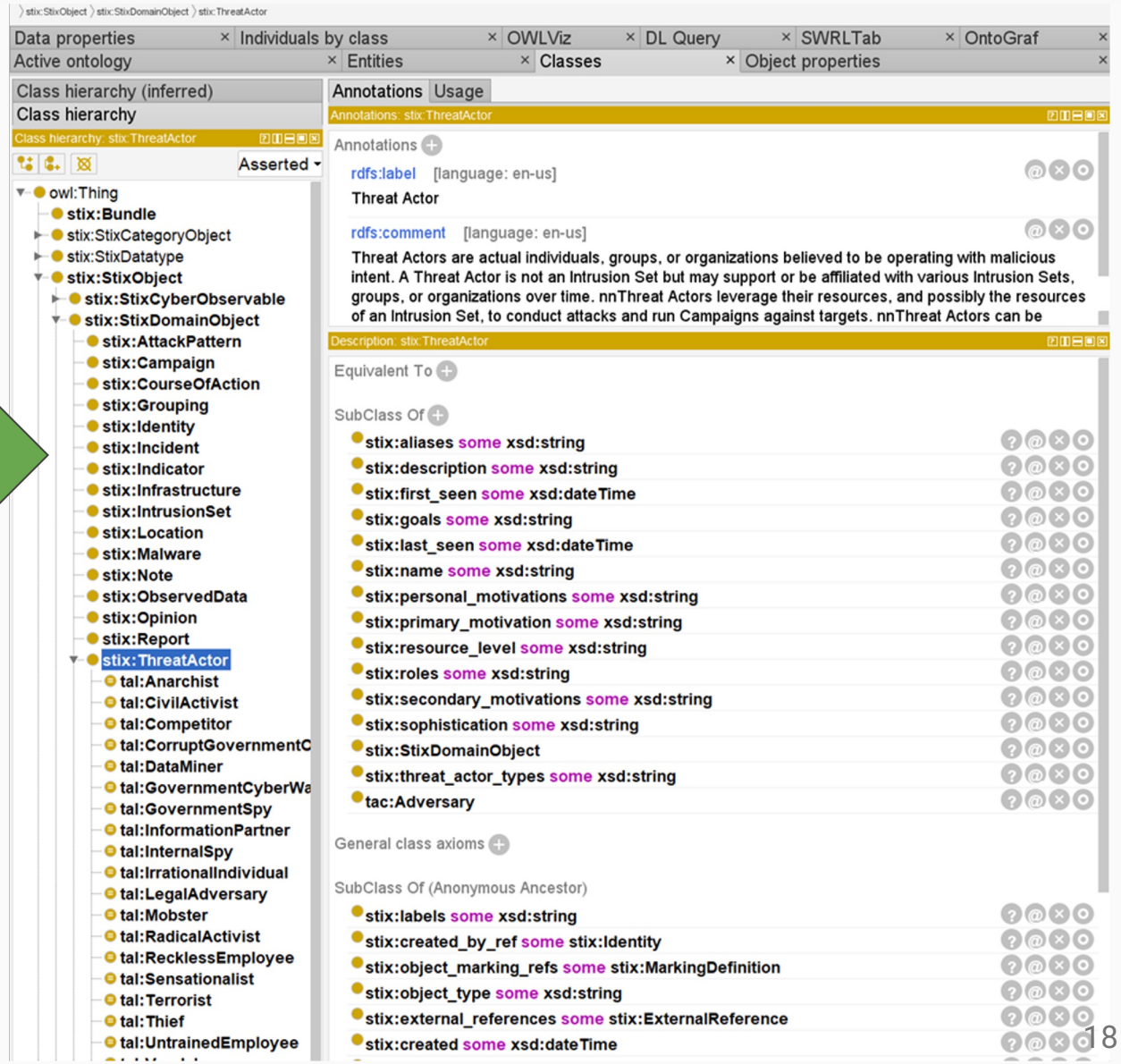
Chairs:
Richard Struse (rjs@mitre.org), MITRE Corporation
Trey Darley (trey.darley@cert.be), CCB/CERT.be

Editors:
Bret Jordan (bret.jordan@broadcom.com), Broadcom
Rich Piazza (rpiazza@mitre.org), MITRE Corporation
Trey Darley (trey.darley@cert.be), CCB/CERT.be

Related work:
This specification replaces or supersedes:
- *STIX Version 2.0. Part 1: STIX Core Concepts.* Edited by Rich Piazza, John Wunder, and Bre
- *STIX Version 2.0. Part 2: STIX Objects.* Edited by Rich Piazza, John Wunder, and Bret Jorda
- *STIX Version 2.0. Part 3: Cyber Observable Core Concepts.* Edited by Ivan Kirillov and Trey
- *STIX Version 2.0. Part 4: Cyber Observable Objects.* Edited by Ivan Kirillov and Trey Darley.
- *STIX Version 2.0. Part 5: STIX Patterning.* Edited by Ivan Kirillov and Trey Darley. Latest stag

This specification is related to:
- *TAXII Version 2.1.* Edited by Bret Jordan and Drew Varner. Latest stage: https://docs.oasis-op
- *STIX/TAXII 2.0 Interoperability Test Document: Part 1 Version 1.1.* Edited by Allan Thomson
  v1.1.html.
- *STIX/TAXII 2.0 Interoperability Test Document: Part 2 Version 1.0.* Edited by Allan Thomson
  v1.0.html.

TAC Conversion Software



stix:StixObject › stix:StixDomainObject › stix:ThreatActor

Data properties | Individuals by class | OWLViz | DL Query | SWRLTab | OntoGraf
Active ontology | Entities | Classes | Object properties

Class hierarchy (inferred)
Class hierarchy
Class hierarchy: stix:ThreatActor
Asserted

- owl:Thing
  - stix:Bundle
  - stix:StixCategoryObject
  - stix:StixDatatype
  - stix:StixObject
    - stix:StixCyberObservable
    - stix:StixDomainObject
      - stix:AttackPattern
      - stix:Campaign
      - stix:CourseOfAction
      - stix:Grouping
      - stix:Identity
      - stix:Incident
      - stix:Indicator
      - stix:Infrastructure
      - stix:IntrusionSet
      - stix:Location
      - stix:Malware
      - stix:Note
      - stix:ObservedData
      - stix:Opinion
      - stix:Report
      - stix:ThreatActor
        - tal:Anarchist
        - tal:CivilActivist
        - tal:Competitor
        - tal:CorruptGovernmentC
        - tal:DataMiner
        - tal:GovernmentCyberWa
        - tal:GovernmentSpy
        - tal:InformationPartner
        - tal:InternalSpy
        - tal:IrrationalIndividual
        - tal:LegalAdversary
        - tal:Mobster
        - tal:RadicalActivist
        - tal:RecklessEmployee
        - tal:Sensationalist
        - tal:Terrorist
        - tal:Thief
        - tal:UntrainedEmployee

Annotations | Usage
Annotations: stix:ThreatActor

Annotations
rdfs:label [language: en-us]
Threat Actor

rdfs:comment [language: en-us]
Threat Actors are actual individuals, groups, or organizations believed to be operating with malicious intent. A Threat Actor is not an Intrusion Set but may support or be affiliated with various Intrusion Sets, groups, or organizations over time. nnThreat Actors leverage their resources, and possibly the resources of an Intrusion Set, to conduct attacks and run Campaigns against targets. nnThreat Actors can be

Description: stix:ThreatActor

Equivalent To

SubClass Of
- stix:aliases some xsd:string
- stix:description some xsd:string
- stix:first_seen some xsd:dateTime
- stix:goals some xsd:string
- stix:last_seen some xsd:dateTime
- stix:name some xsd:string
- stix:personal_motivations some xsd:string
- stix:primary_motivation some xsd:string
- stix:resource_level some xsd:string
- stix:roles some xsd:string
- stix:secondary_motivations some xsd:string
- stix:sophistication some xsd:string
- stix:StixDomainObject
- stix:threat_actor_types some xsd:string
- tac:Adversary

General class axioms

SubClass Of (Anonymous Ancestor)
- stix:labels some xsd:string
- stix:created_by_ref some stix:Identity
- stix:object_marking_refs some stix:MarkingDefinition
- stix:object_type some xsd:string
- stix:external_references some stix:ExternalReference
- stix:created some xsd:dateTime

Extended Classification Schema - Tim Casey's (INTEL) Threat Agent Library

What are the defining characteristics of a Competitor?

Description: tal:Competitor

Equivalent To

stix:ThreatActor
and (tac:categorizedBy value tal:AdeptSkills)
and (tac:categorizedBy value tal:BusinessAdvantageOutcome or tac:categorizedBy value tal:TechnologyAdvantageOutcome)
and (tac:categorizedBy value tal:ClandestineVisibility)
and (tac:categorizedBy value tal:CopyObjective)
and (tac:categorizedBy value tal:ExternalAccess)
and (tac:categorizedBy value tal:MinorExtraLegalLimits)

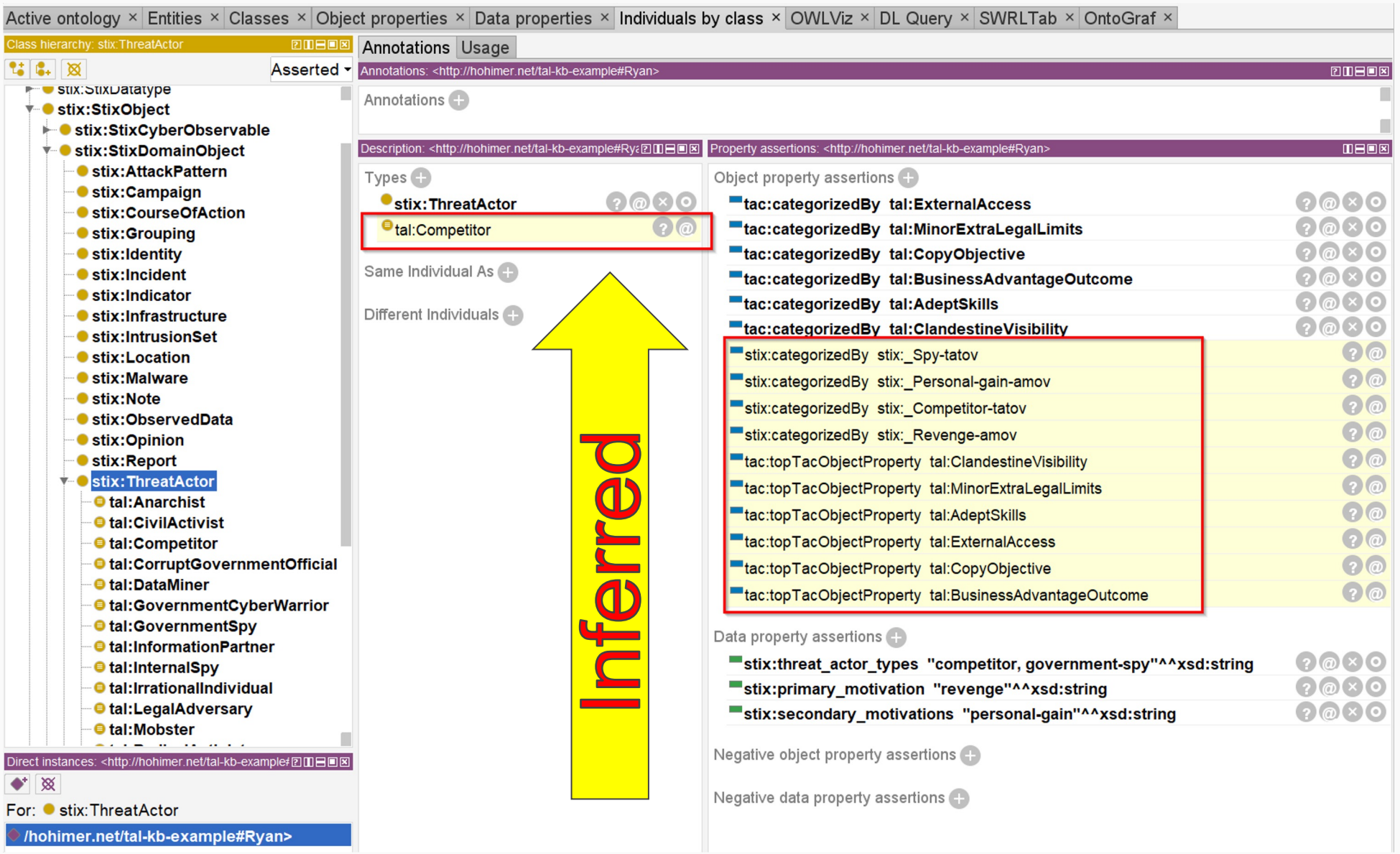
What are the defining characteristics of a Government Cyber Warrior?

Description: tal:GovernmentCyberWarrior

Equivalent To

stix:ThreatActor
and (tac:categorizedBy value tal:AdeptSkills)
and (tac:categorizedBy value tal:AnyVisibility)
and (tac:categorizedBy value tal:CopyObjective or tac:categorizedBy value tal:DenyObjective or tac:categorizedBy value tal:DestroyObjective)
and (tac:categorizedBy value tal:DamageOutcome or tac:categorizedBy value tal:EmbarrassmentOutcome)
and (tac:categorizedBy value tal:ExternalAccess)
and (tac:categorizedBy value tal:GovernmentResources)
and (tac:categorizedBy value tal:MajorExtraLegalLimits)

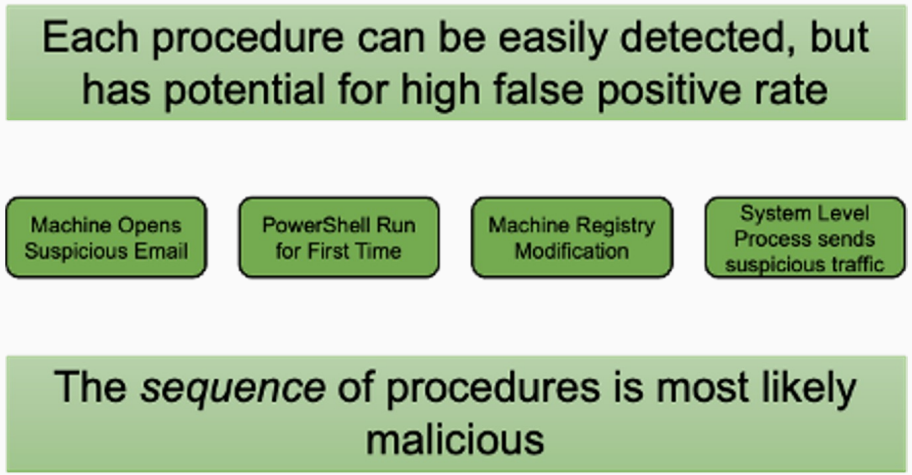
Automated Classification of “Competitor” by Description Logics Reasoning.



IOB Overview

Indicator of Behavior Concept

- Indicator of Behavior (IOB) STIX bundles provide repeatable sets of observed adversary behaviors to help defender tools & capabilities
  - Intelligence context provided in machine-readable graph representation
  - Relationships to relevant ATT&CK attack pattern objects
  - Relationships to detection analytics
  - Includes correlation workflows to address false-positives
  - Includes response COAs and cybersecurity operations playbooks in standardized formats



TAXII Server

- IOB has set up a TAXII server to support sharing STIX bundles during the CASP Village
- Utilizing the OASIS cti-taxii-server, medallion
  - https://github.com/oasis-open/cti-taxii-server

TAXII server available via port 5000 on EC2 instance for plugfest

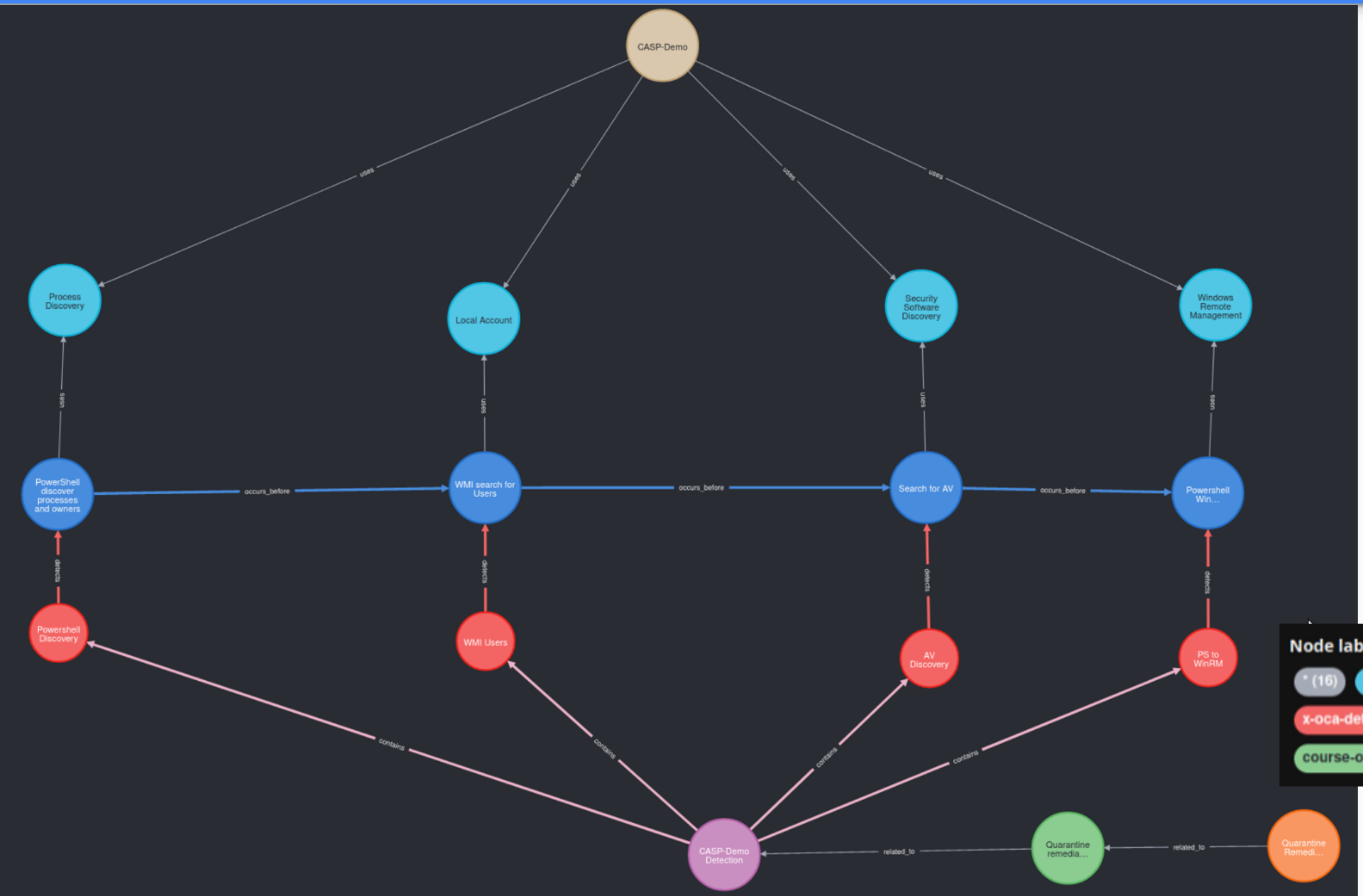
```
[CASP> curl -i http://127.0.0.1:5000/trustgroup1/collections/91a7b528-80eb-42ed-a74d-c6f
bd5a26116/objects/ -u    credentials   -H "Accept: application/taxii+json;version=2.1" |
sed '10p;d' | python3 -m json.tool
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1849  100  1849    0     0   112k      0 --:--:-- --:--:-- --:--:--  120k
{
    "more": false,
    "objects": [
        {
            "created": "2014-05-08T09:00:00.000Z",
            "id": "relationship--2f9a9aa9-108a-4333-83e2-4fb25add0463",
            "modified": "2014-05-08T09:00:00.000Z",
            "relationship_type": "indicates",
            "source_ref": "indicator--cd981c25-8042-4166-8945-51178443bdac",
            "spec_version": "2.1",
            "target_ref": "malware--c0931cc6-c75e-47e5-9036-78fabc95d4ec",
            "type": "relationship"
        },
        {
            "created": "2014-05-08T09:00:00.000Z",
            "id": "indicator--cd981c25-8042-4166-8945-51178443bdac",
            "indicator_types": [
                "file-hash-watchlist"
            ],
            "modified": "2014-05-08T09:00:00.000Z",
            "name": "File hash for Poison Ivy variant",
            "pattern": "[file:hashes.'SHA-256' = 'ef537f25c895bfa782526529a9b63d97aa631
564d5d789c2b765448c8635fb6c']",
            "pattern_type": "stix",
            "spec_version": "2.1",
            "type": "indicator",
            "valid_from": "2014-05-08T09:00:00.000000Z"
        },
```

STIX2NEO4J Script

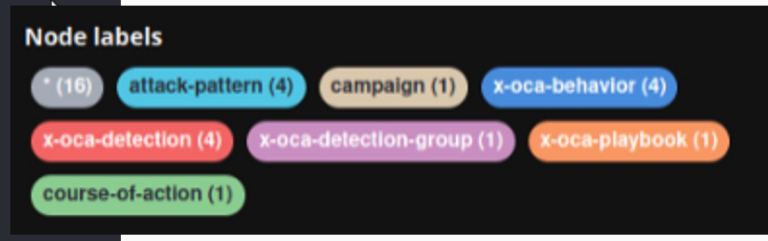
- Python script for analyzing STIX 2.x bundles in a neo4j graph database
- Provides additional analytical capabilities for investigating raw STIX messages without major modification of the data
- Threat Intel Platforms often make significant changes to data model upon import
- Released on an Apache2 license through the Open Cybersecurity Alliance Indicator of Behavior Sub-Project
- Script repository link on GitHub:
  - https://github.com/opencybersecurityalliance/oca-iob/tree/main/STIX2NEO4J%20Converter

Converter and Neo4J database available on EC2 instance for plugfest

Sample IOB Bundle for CASP Village



- **IOB** behaviors in behavior SDOs
- **ATT&CK** info in Attack Pattern SDOs from MITRE
- Detection Objects with **Stix-Shifter** queries
- Detection Group with **Kestrel** correlation
- Playbook object with **CACAO** workflow



STIX Shifter Queries Embedded in IOB Bundle

	DetectionName	AnalyticType	AnalyticRule
1	"Powershell Discovery"	"Stix-Shifter Query - base64 encoded text"	"# TTP: Find user processes (T1057) t1057_instances = GET process FROM stixshifter://bh22-windows-192.168.56.111 WHERE name = 'powershell.exe' AND command_line LIKE '%getowner%get-process%' START 2022-07-01T00:00:00Z STOP 2022-08-01T00:00:00Z DISP t1057_instances ATTR pid, name, command_line"

Kestrel Huntbook Embedded in IOB Bundle

	A.name	A.description	Corr_Type	Corr_Note	Corr_Workflow

1	"CASP-Demo Detection"	"This Detection Group finds the behaviors within the CASP Demo."	"Kestrel - base64 encoded HuntBook"	"Decode base64 string and save as .ipynb Jupyter Notebook"	"{
					"cells": [
					{
					"cell_type": "markdown",
					"id": "e09a7ee5",
					"metadata": {},
					"source": [
					"## Known Facts\n",
					"\n",
					"- `192.168.56.111`\n",
					" - Windows 10\n",
					" - Employee's laptop\n",
					" - Company email client: `WinMail.exe`\n",
					" - [Sysmon](https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon) -> [Elasticsearch](https://www.elastic.co/) in the cloud\n",
					" - Entire data is accessible through [stix-shifter](https://github.com/opencybersecurityalliance/stix-shifter)\n",
					" - Partial data dumped for this demo\n",
					" - stix-shifter data source name in this hunt: `bh22-windows-192.168.56.111`\n",
					"- `192.168.56.112`\n",
					" - Windows 10\n",
					" - Developer's desktop\n",
					" - Windows Remote Desktop and Remote Management enabled\n",
					" - [Sysmon](https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon) -> [Elasticsearch](https://www.elastic.co/) in the cloud\n",
					" - stix-shifter data source name in this hunt: `bh22-windows-192.168.56.112`\n",
					"- `192.168.56.91`\n",
					" - Linux 5.10 server with containers running\n",
					" - Enterprise's internal web service (`NodeJS`)\n",
					" - [Sysflow](https://github.com/sysflow-telemetry) -> [Elasticsearch](https://www.elastic.co/) in the cloud\n",
					" - stix-shifter data source name in this hunt: `bh22-linux-192.168.56.91`"
					]
					},
					{
					"cell_type": "markdown",
					"id": "d09ff33d",
					"metadata": {},
					"source": [
					"## Where to Start?\n",
					"\n",
					"How about TTPs specified in [MITRE](https://www.mitre.org/) [CALDERA](https://caldera.mitre.org/)?\n",
					"\n",
					"![CALDERA T1057](images/caldera_overview_n_T1057.png)"
					]
					},
					{
					"cell_type": "code",
					"execution_count": 1,
					"id": "15f340b8",
					"metadata": {},

CACAO Response Workflow in IOB Bundle

```
neo4j$ //Show the CACAO Playbook Data (Requires APOC enabled on NEo4j) MATCH (A:`x-oca-playbook`)-[r]→(B:`course-of-action`) WHERE A.bundlesource="CASPDEMO" RETURN A.name,A…
```

Table | Text | Code

	A.name	A.playbook_type	A.playbook_format	apoc.text.base64Decode(A.playbook_bin)	type(r)	B.name

1	"Quarantine and Remediate"	"remediation"	"CACAO"	"{
				"type": "playbook",
				"spec_version": "cacao-2.0",
				"id": "playbook--767d859e-7387-4e0c-95c0-458ca369486f",
				"name": "Process_1811f8w: Quarantine and Remediate",
				"playbook_types": [
				"mitigation",
				"remediation"
				],
				"created_by": "identity--b085a68a-bf48-4316-9667-37af78cba894",
				"created": "2022-03-31T13:00:00.000Z",
				"modified": "2022-03-31T13:00:00.000Z",
				"workflow_start": "start--ece532df-970a-417c-a125-5e7713e10f7c",
				"workflow": {
				"start--ece532df-970a-417c-a125-5e7713e10f7c": {
				"name": "StartEvent_1: System Course of Action Alert",
				"on_completion": "action--d22408fc-a99c-4c45-8770-27dac6df293a",
				"type": "start"
				},
				"end--4d3134d9-68d2-4bde-87ca-a5bfe8468aa6": {
				"name": "Event_17zpsn5: End",
				"type": "end"
				},
				"action--d22408fc-a99c-4c45-8770-27dac6df293a": {
				"name": "Activity_1vv8yyz: Quarantine system",
				"on_completion": "action--d1d15ab7-b557-4f82-8d9b-495438a5c9a9",
				"type": "action",
				"commands": [
				{
				"type": "http-api"
				}
				]
				},
				"action--d1d15ab7-b557-4f82-8d9b-495438a5c9a9": {
					"related_to"	"Quarantine and remediate"

PACE Overview

Posture Attribute Collection & Evaluation

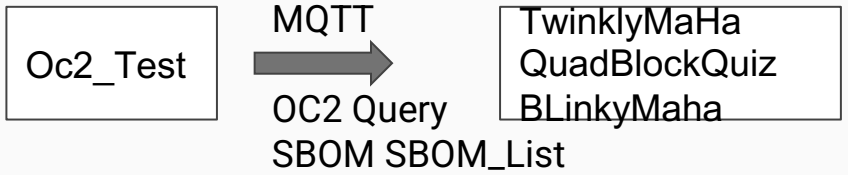
PACE

- https://opencybersecurityalliance.org/pace/
- https://github.com/opencybersecurityalliance/PACE/tree/main/docs/UseCases/Pace_Sbom_Vex_Flags_Prioritization
- https://securityattributes.org/By_Example/
- Commercial Vendors
- Gartner Application Security Posture Managment

SBOM Overview

Software Bill of Materials

- https://www.cisa.gov/sbom
- https://twinklymaha-prod-q353uyxfhq-uk.a.run.app/.well-known/sbom
- https://quadquiz-q353uyxfhq-uk.a.run.app/.well-known/sbom
- SBOMarama tomorrow



VEX Overview

Vulnerability Exploitability eXchange (VEX)

Vex & csaf summit

QBQ link

Conclusion

- Successful event showcasing the use of open standards and tools working together to enable advanced cyber defense

- Next village is being scheduled
  - 2-day Village in 1Q24
  - NJ or DC
  - Host Negotiations in progress